
ALCALDÍA DE PASTO

ALCALDÍA DE PASTO

SECRETARÍA GENERAL

SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ELABORACIÓN, REVISIÓN Y APROBACIÓN DE DOCUMENTOS		
DATOS	AJUSTADO POR	REVISADO POR
FIRMA		
NOMBRE	MIGUEL EDUARDO GUERRERO IBARRA	RAÚL ALBERTO CHAVES SÁNCHEZ
CARGO	Contratista	Subsecretario de Sistemas de Información

CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Estructuración Modelo de Seguridad y Privacidad de la Información		

APROBACIÓN COMITÉ MIPG.

NO. DE ACTA	FECHA

Contenido

INTRODUCCIÓN

EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI como su nombre bien lo dice es un modelo que se compone de un conjunto de 21 Guías con las cuales la Alcaldía debe incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de

preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El MSPI se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en Alcaldía, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.

JUSTIFICACION

El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, La Alcaldía Municipal de Pasto a través de la Subsecretaria de Sistemas de Información dando cumplimiento a sus funciones implementa El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.
Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la

información con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la Alcaldía, todo esto acorde con lo expresado en la legislación Colombiana.

DEFINICIONES

1. **Acceso a la Información Pública:**

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

2. **Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

3. **Activo de Información:**

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad.

4. **Archivo:**

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Alcaldía pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

5. **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

6. **Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

7. **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

8. **Autorización:**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

9. **Bases de Datos Personales:**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

10. **Ciberseguridad**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

11. **Ciberespacio**

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

12. **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo

del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

13. Datos Abiertos

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las empresas públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan

Reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

14. Datos Personales:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

15. Datos Personales Públicos:

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

16. Datos Personales Privados:

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

17. Datos Personales Mixtos:

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

18. Datos Personales Sensibles:

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

19. Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

20. Derecho a la Intimidad:

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

21. Encargado del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

22. Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

23. Información Pública Clasificada:

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

24. Información Pública Reservada:

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

25. Ley de Habeas Data:

Se refiere a la Ley Estatutaria 1266 de 2008.

26. Ley de Transparencia y Acceso a la Información Pública:

Se refiere a la Ley Estatutaria 1712 de 2014.

27. Mecanismos de protección de datos personales:

Lo constituyen las distintas alternativas con que cuentan la Alcaldíadestinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

28. Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

29. Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

30. Privacidad:

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Alcaldía en el marco de las funciones que a ella le compete realizar y que generan en la Alcaldíadestinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

31. Registro Nacional de Bases de Datos:

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

32. Responsabilidad Demostrada:

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

33. Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

34. Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

35. Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

36. Titulares de la información:

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

37. Tratamiento de Datos Personales:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

38. Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Alcaldía. (ISO/IEC 27000).

39. Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

40. Partes interesadas (Stakeholder)

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

OBJETIVOS

OBJETIVO GENERAL

Implementar un conjunto de buenas prácticas en función de un adecuado ciclo de vida de la seguridad y privacidad de la información alineadas con la NTC/IEC ISO 27001:2013, la estrategia de gobierno digital, la Política de Seguridad Digital y Continuidad del servicio, en cumplimiento de las disposiciones legales vigentes.

OBJETIVOS ESPECIFICOS

- Mantener los lineamientos que se establezcan con respecto al manejo de la información física y/o digital en función de tener una gestión documental basada en Seguridad y Privacidad de la Información.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación en la Alcaldía Municipal de Pasto.

- Mitigar incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
- Promover el uso de mejores prácticas de seguridad de la información.
- Optimizar la gestión de la seguridad y privacidad de la información al interior de la Alcaldía Municipal de Pasto.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal

ALCANCE

Toda la Alcaldía Municipal de Pasto y cualquier tipo de persona que haga uso de sus recursos o información.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de la Alcaldía Municipal de Pasto adoptara las 5 fases en función de lograr una adecuada gestión de la seguridad y privacidad de sus activos de información.

De igual manera contemplara los 6 niveles de madurez correspondientes a la evolución de la implementación del MSPI en la Alcaldía Municipal de Pasto.

Este componente transversal de la estrategia de gobierno digital se alineara al componente TIC para la gestión y estará enfocado a preservar la confidencialidad, integridad y disponibilidad de la información contribuyendo así al cumplimiento de la misión y objetivos estratégicos de la Alcaldía Municipal de Pasto.

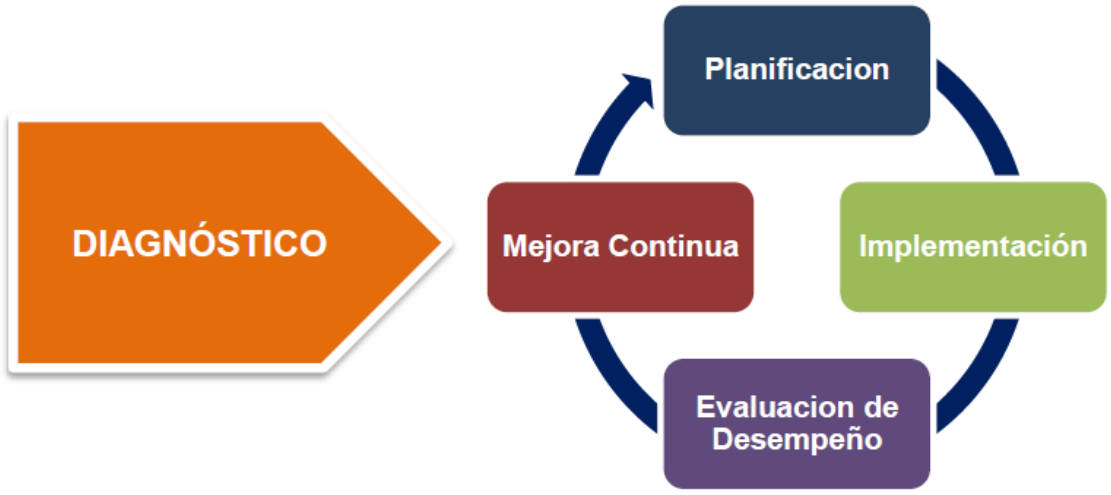
El MSPI de la Alcaldía Municipal de Pasto también se alineara al componente TIC para servicios apoyando todo aquel proceso en el cual exista tratamiento de información en los trámites y servicios ofrecidos garantizando en cumplimiento de la ley el acceso a determinada información.

De esta manera se contara con un servicio más transparente, colaborativo y participativo al garantizar información con controles de seguridad y privacidad.

DESCRIPCION DEL CICLO DE OPERACIÓN

En el presente capitulo se describe ciclo de operación a través de una descripción detallada de cada una de las cinco (5) fases que lo comprende.

Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información.



Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Fase de diagnóstico – Etapas previas a la implementación

En esta etapa se identificara el estado actual de la Alcaldía Municipal de Pasto con respecto a los requerimientos del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Figura 2. Etapas previas a la implementación

Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Estado actual de la Alcaldía

Para determinar el estado actual de la Alcaldía, se utiliza el INSTRUMENTO DE IDENTIFICACIÓN DE LINEA BASE DE SEGURIDAD con el cual se establece el estado actual y/o avance de implementación con respecto al ciclo de operación más específicamente la efectividad de los controles que se tengan implementados, las brechas al anexo ISO27001:2013, en que estado se encuentra el avance del

ciclo de funcionamiento del modelo de operación (PHVA) y el nivel de madurez del modelo de seguridad y privacidad de la información

Con respecto a lo anterior se tiene en cuenta la tabla 1 de la Guía Modelo de Seguridad y Privacidad de la información en la cual se especifica las metas, Resultados e Instrumentos de la fase etapas previas a la implementación.

Tabla 1. Metas, Resultados e Instrumentos de la fase etapas previas a la implementación.

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Los resultados de la aplicación de la herramienta para la identificación de nivel de madurez de la Alcaldía se presentan como anexo al documento debido a su extensión y estructura.

PRUEBAS DE EFECTIVIDAD

En esta fase la Alcaldía Municipal de Pasto debe identificar los riesgos que se manifiestan a través de las debilidades en la implementación del modelo de seguridad y privacidad de la información y las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos.

Estas pruebas están orientadas a evaluar la estructura de seguridad en la Alcaldía y para esto la Alcaldía Municipal de Pasto debe revisar varios frentes de trabajo, como son el anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel de madurez de la Alcaldía de acuerdo a los niveles expuestos en el modelo de seguridad y privacidad y recomendaciones para se llegue a plasmar el concepto de Ciberseguridad.

Levantamiento de información

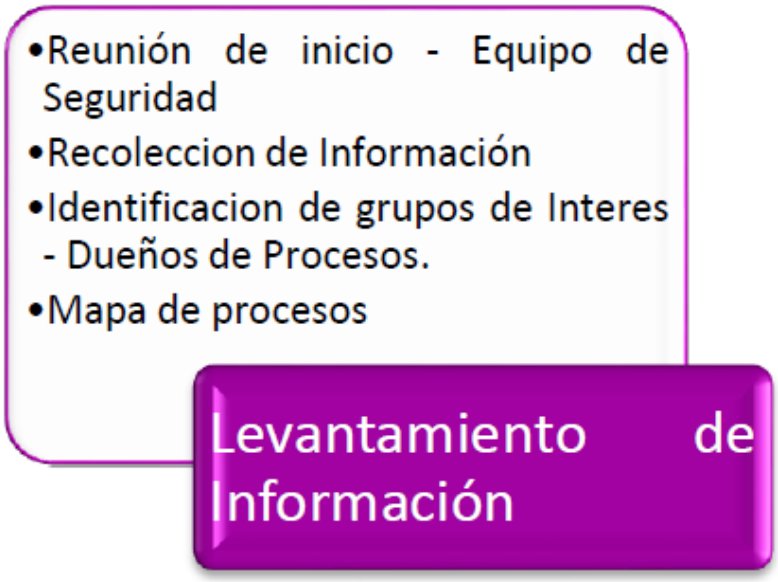
En esta fase la Alcaldía debe recopilar la información necesaria para iniciar la actividad, dicha información puede ser organizada por parte del equipo de seguridad de la información de la Alcaldía Municipal de Pasto o quien haga sus veces como equipo.

La información recogida no solo debe permitir identificar los activos más importantes de la Alcaldía, relacionados con los procesos de la misma, ya sea misionales o de apoyo, También me debe permitir el conocer el contexto de la Alcaldía, es decir, el entorno donde se proyectan los objetivos de la Alcaldía.
El grupo de personas que hace la recolección de información, debe reconocer el organigrama de la Alcaldía, mapa de procesos, política de seguridad, manual de

políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la Alcaldía.

En esta fase también se debe identificar los grupos de interés, al interior de la Alcaldía, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, líderes de procesos.

Figura 3. Levantamiento de Información



Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

IDENTIFICACIÓN DE AMENAZAS

La identificación de amenazas no es otra cosa que la evaluación del riesgo que se realiza en la Alcaldía, es decir, es la evaluación de las actividades donde se ven involucradas las personas, la infraestructura y los procesos; con el objetivo de identificar las amenazas que se ciernen sobre la Alcaldía.

El resultado de estas actividades permite desarrollar planes de mitigación para las vulnerabilidades encontradas, orientar mejor los recursos y la ayuda a las áreas de la Alcaldía que más lo requieren; la búsqueda de estas amenazas debe ser desde que se crean los procesos y durante su ciclo de vida.

Estas actividades deben tener un enfoque simple, es decir, descomponer los procesos a través de la evaluación manual, de manera que se sepa cómo funciona y su interrelación con las otras actividades.

- Definir y clasificar los activos de la Alcaldía, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
- Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
- Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasma los análisis de riesgo de la Alcaldía y sus planes de mitigación a través de los controles sugeridos

Para el levantamiento de la información, se puede apoyar en el instrumento de diagnóstico y seguimiento que ha puesto a disposición de la Alcaldíael Ministerio TIC.

PRUEBAS Y ANÁLISIS

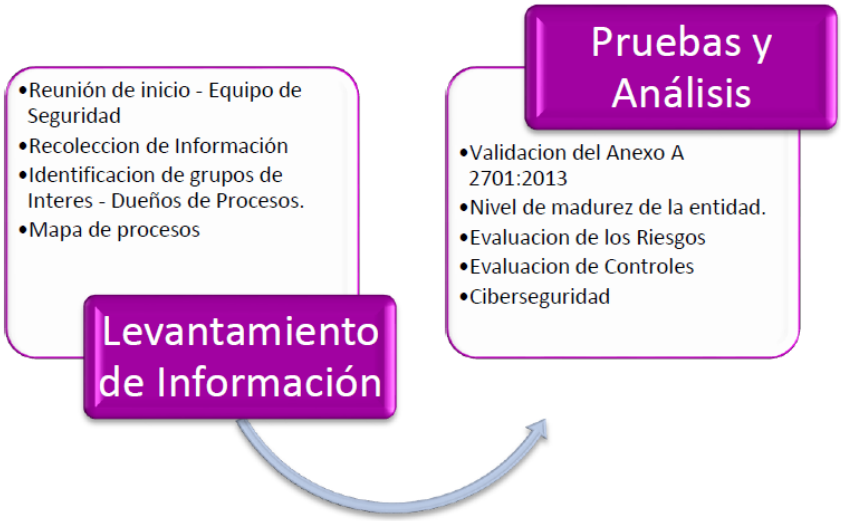
En esta fase las Alcaldía identificara los riesgos que se manifiestan a través de las debilidades en la implementación del modelo de seguridad y privacidad de la

información y las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos.

Estas pruebas están orientadas a evaluar la estructura de seguridad en la Alcaldía.

Para esto la Alcaldíadeben revisar varios frentes de trabajo, como son el anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel de madurez de la Alcaldía de acuerdo a los niveles expuestos en el modelo de seguridad y privacidad y recomendaciones para que la Alcaldía llegue a plasmar el concepto de Ciberseguridad.

Figura 4. Componentes levantamiento de información y Pruebas de Análisis



Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Las pruebas de vulnerabilidad en resumen son unas técnicas empleadas para comprobar la seguridad de una Alcaldía. Las pruebas son esencialmente las pruebas sobre aplicaciones, procesos y usuarios para encontrar vulnerabilidades.

Actualmente se encuentran diferentes técnicas y el cuándo usarlas, las cuales son necesarias para tener un marco de referencia del nivel de seguridad en el que se esta evaluando; así como tampoco hay una sola técnica que cubra todas las comprobaciones necesarias para evaluar todo lo requerido por la Alcaldía.

Una orientación objetiva al realizar la evaluación, le permite a la Alcaldía de manera equitativa realizar actividades manuales como pruebas técnicas; esto dará como resultado la posibilidad de una comprobación completa de lo avanzado en la implementación del modelo de seguridad y privacidad.

Para entender mejor esta fase, tenga presente las siguientes recomendaciones metodológicas con las cuales se busca proteger la disponibilidad, integridad, y confidencialidad de la información.

TIPOS DE PRUEBAS DE EFECTIVIDAD

Pueden realizarse 3 tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o infraestructura de la Alcaldía objetivo:

- **Pruebas Con Conocimiento Nulo Del Entorno:** Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco o nulo conocimiento del objetivo o su infraestructura.

- **Pruebas Con Conocimiento Medio Del Entorno:** Es cuando para la prueba de pentesting, se tiene más información sobre el ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc… pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.

- **Pruebas Con Conocimiento Completo Del Entorno:** Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.

ALCANCE DE LAS PRUEBAS

Deben existir reglas específicas para la ejecución de las pruebas de efectividad técnicas, para asegurar que dichas actividades no incurran en fallas mayores y se pueda afectar la infraestructura o las operaciones de la Alcaldía. Dentro del alcance se pueden definir los siguientes aspectos:

- **Plan De Trabajo:** Debe definirse durante cuánto tiempo se realizarán las pruebas, los sistemas que harán parte de las pruebas, las actividades específicas, los procedimientos de contingencia en caso de alguna afectación etc….

- **Insumos:** Que recursos son necesarios para realizar las actividades: Personal adicional, ventanas de tiempo, equipos etc…

- **Responsables:** Quienes serán los encargados de efectuar las pruebas (sean proveedores o funcionarios de la Alcaldía).

- **Afectaciones Posibles:** El tipo de afectación que puede llegar a darse sobre cada sistema, también debe definirse si el objetivo es realizarlo en horario de producción o en horario de baja actividad laboral.

- **Multas o Sanciones:** En caso de incumplir los parámetros anteriormente mencionados, deberán fijarse las sanciones disciplinarias o multas.

PROCEDIMIENTO DE EJECUCIÓN DE PRUEBAS DE EFECTIVIDAD

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial

Figura 5. Ciclo para la ejecución de pruebas de efectividad técnicas.

Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Para ampliar más lo correspondiente al apartado pruebas de efectividad la Alcaldía Municipal de Pasto debe consultar e implementar lo considerado de la

Guia N1. METODOLOGIA PRUEBAS DE EFECTIVIDAD del MSPI.

FASE DE PLANIFICACION

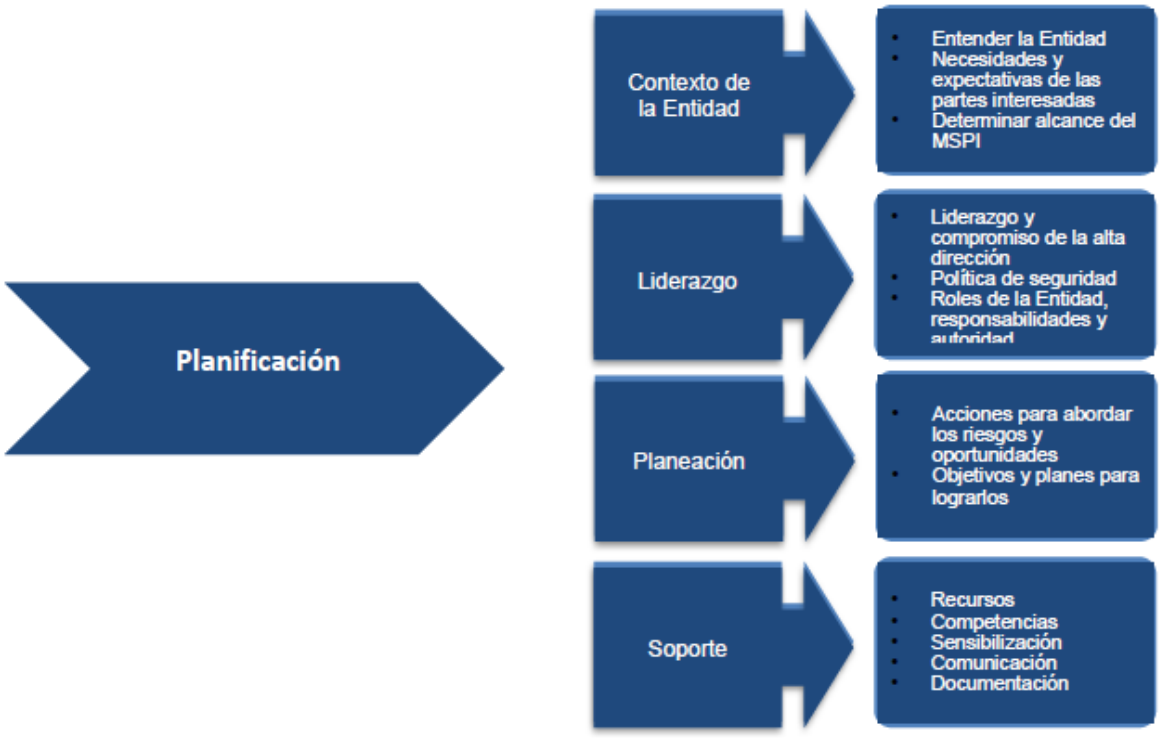
Para el desarrollo de esta fase la Alcaldía debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la Alcaldía, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permitirá a la Alcaldía definir los límites sobre los cuales se implementará la seguridad y privacidad en la Alcaldía.

Este enfoque es por procesos y debe extenderse a toda la Alcaldía.

Para desarrollar el alcance y los límites del Modelo se debera tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

Figura 6. Fases de planificación[i]



Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

Es importante tener en cuenta la siguiente tabla que se adopta del Modelo de Seguridad y Privacidad de la Información emitido por el MINTIC para un mejor control del cumplimiento de la Fase.

Tabla 2. Metas y Resultados Fase de Planificación

Planificación			
Metas	**Resultados**	**INSTRUMENTOS MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestion Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Guía No 7 - Gestion de Riesgos Guía No 8 - Controles de Seguridad	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

POLITICAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

ALCANCE

Esta política aplica a toda la Alcaldía, sus servidores públicos de planta, contratistas y terceros de la ALCALDÍA DE PASTO y la ciudadanía en general que tenga contacto con la Alcaldía.

DEFINICIONES

- ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, Alcaldías o procesos autorizados.

- DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una Alcaldía autorizada, cuando ésta así lo requiera.

- INFORMACIÓN: Datos relacionados que tienen significado para la Alcaldía. La información es un activo que, como otros activos importantes para la Alcaldía, es esencial para las actividades de la Alcaldía y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

- INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

- POLÍTICA: Declaración de alto nivel que describe la posición de la Alcaldía sobre un tema específico.

- SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ALCALDÍA DE PASTO, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Alcaldía.

Para la ALCALDÍA DE PASTO, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Alcaldía según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la Alcaldía.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la ALCALDÍA DE PASTO.
- Garantizar la continuidad del negocio frente a incidentes.
- La ALCALCÍA DE PASTO ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Alcaldía, y a los requerimientos regulatorios.

NIVELES DE APLICACIÓN DE LA POLÍTICA

1. PRIMER NIVEL: Definidas en el presente documento.

2. SEGUNDO NIVEL: Definidas en un documento cuyo nombre será: Manual de políticas de Seguridad de la Información de segundo nivel, este documento deberá ser formalizado en el sistema de gestión de calidad, en el proceso de Gestión de Tecnologías de la Información.

A continuación, se establecen las 12 políticas de seguridad que soportan el Sistema de Seguridad y Privacidad de la Información de la ALCALDÍA DE PASTO:

1. La ALCALDÍA DE PASTO ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades de la Alcaldía, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. La ALCALDÍA DE PASTO protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.
4. La ALCALDÍA DE PASTO protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. La ALCALDÍA DE PASTO protegerá su información de las amenazas originadas por parte del personal.

6. La ALCALDÍA DE PASTO protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. La ALCALDÍA DE PASTO controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. La ALCALDÍA DE PASTO implementará control de acceso a la información, sistemas y recursos de red.

9. La ALCALDÍA DE PASTO garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. La ALCALDÍA DE PASTO garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. La ALCALDÍA DE PASTO garantizará la disponibilidad de sus procesos y la continuidad de su operación basado en el impacto que pueden generar los eventos.

12. La ALCALDÍA DE PASTO garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política general de Seguridad y Privacidad de la Información o de las políticas de seguridad de la información de segundo nivel, traerá consigo, las consecuencias legales que apliquen a la normativa de la Alcaldía, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la Información se refiere a lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la Información se refiere.

Políticas de dispositivos móviles institucionales

La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

Políticas de seguridad de los recursos humanos

Para el caso de contratación directa de personal, será el supervisor del contrato y el Departamento Administrativo de Contratación Pública realizaran las verificaciones de los antecedentes (procuraduría, contraloría, policía) de la persona idónea aspirante al contrato, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

Para el caso de personal de planta que se vincule a la entidad será la subsecretaría de Talento Humano la encargada de verificar los antecedentes del aspirante al cargo cumpliendo la normatividad respectiva vigente.

Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.

La Entidad establece directrices para asegurar que los servidores públicos tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información.

Los acuerdos contractuales o funciones asignadas a los servidores públicos especifican el cumplimiento a los lineamientos de seguridad de la información establecidos en la Entidad.

El proceso de Talento Humano y/o contratación realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada a los administradores de sistemas de información institucional o quien haga sus veces con el fin de que se realice la respectiva finalización de membresías de acceso a que haya lugar.

La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, acarreará las sanciones a que haya lugar.

Políticas gestión de activos

La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

Políticas control de acceso

La Entidad define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataformas tecnológicas, considerándolas importantes para el sistema de gestión de seguridad de la información.
La Entidad establece procedimientos para la creación de datos de acceso, suministro de accesos a la información, revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual o laboral.
Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.
Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

Política de controles criptográficos

El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa, será a través de conexiones seguras.
Se deberán cifrar o aplicar claves a los documentos (pdf, Excel, Word, bd, csv, etc.) que contengan datos personales o datos sensibles.

Políticas de seguridad física y del entorno

Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos:
a. Al momento de retirar un equipo en la organización (almacén), el proceso de TI realiza una copia de respaldo de la información almacenada en este activo.
b. El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.
c. Los servidores públicos, garantizan que no se disponga información de la Entidad en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.

d. Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

e. Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

Políticas seguridad en las operaciones

La Entidad documenta los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.
Según la clasificación de la información establecida por la Entidad, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento.

Los responsables de los sistemas de información de mayor criticidad definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.

Políticas seguridad de las comunicaciones

El Proceso de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

Políticas adquisición, desarrollo y mantenimiento de sistemas

La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

Políticas relaciones con los proveedores

Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que proveedor contratado puedan responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

La Entidad controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.

Políticas gestión de incidentes en seguridad

La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

La Entidad debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
La Entidad cuenta con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Políticas cumplimiento

La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.
La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

ROLES Y RESPONSABILIDADES

Considerando que la seguridad de la información es un tema transversal a la Alcaldía, y que se hace necesario la participación de todas las áreas, se establecen los roles y responsabilidades del sistema de seguridad de la información, los cuales deben incluir responsables para:

Responsable de Seguridad de la Información para la Alcaldía

El Responsable de Seguridad de la información será el líder del sistema y tendrá las siguientes responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias de la seguridad de la información, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la Alcaldía.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Gestionar el equipo de trabajo de seguridad de la información, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.
- Encarrilar las actividades del sistema hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la Alcaldía.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del sistema para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del sistema de seguridad de la información en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.

- Asegurar la calidad de los entregables y del sistema de seguridad de la información en su totalidad.
- Velar por el mantenimiento de la documentación del sistema de seguridad de la información, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el sistema de seguridad de la información en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del sistema de seguridad de la información.
- Proponer la actualización de las políticas de seguridad de la información.

Equipo de trabajo

Teniendo en cuenta la naturaleza de la Alcaldía, debe conformarse un equipo para el desarrollo del sistema de seguridad de la información al cual deben pertenecer miembros directivos, con el propósito de asegurar que toda la información más relevante de la Alcaldía esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la Alcaldía, y que no dependa exclusivamente de la oficina o área de TI, el equipo estará formado así:

- Al menos un representante de la Subsecretaría de Sistemas de Información.
- Al menos un representante de la Oficina de Control Interno.
- Al menos un representante de la Oficina de Planeación de Gestión Institucional.
- Al menos un representante del Sistema de Gestión de Calidad.
- Al menos un representante de la Oficina de Asesoría Jurídica.
- Al menos un representante de la Subsecretaría de Talento Humano.

- Al menos un representante de la Secretaría General.
- Al menos un representante del Departamento Administrativo de Contratación Pública.
- Representantes de las áreas que puedan apoyar en la implementación del sistema de seguridad de la información.

Responsabilidades del equipo del proyecto:

- Apoyar al líder de proyecto al interior de la Alcaldía.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o la instancia establecida como comité de seguridad de la información.
- Revisar y aprobar las políticas de seguridad de la información de segundo nivel.

Comité de Seguridad

Las funciones de este comité serán asumidas por el Comité Institucional de Gestión y Desempeño bajo las disposiciones establecidas para su funcionamiento y deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo,

así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo, las temáticas a tratar en este comité son:

1. Revisar los diagnósticos del estado de la seguridad de la información en la Alcaldía de Pasto de la Alcaldía.
2. Acompañar e impulsar el desarrollo de proyectos de seguridad.
3. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Alcaldía de Pasto.
4. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
5. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
6. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
7. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
8. Promover la difusión y sensibilización de la seguridad de la información dentro de la Alcaldía.
9. Poner en conocimiento de la Alcaldía, los documentos generados al interior del comité que impacten de manera transversal a la misma.
10. Revisar y aprobar la política de primer nivel de seguridad de la información.

INVENTARIO DE ACTIVOS DE INFORMACION

El inventario de activo de información se está llevando a cabo en un proceso que se está fortaleciendo actualmente según lo sustentando en las jornadas de inducción y reinduccion

Integración del MSPI con el Sistema de Gestión documental.

La Alcaldía deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

Para este fin es deber el implementar o apoyarse bajo la guía N°6 Gestión Documental e integrarlo cuando el proceso de implementación del Sistema de Gestión Documental por lo menos alcance el 70%

Identificación, Valoración Y Tratamiento de Riesgos.

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

La información que hace parte de una Alcaldía Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Alcaldía, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida,

entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Alcaldía o de un Estado.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte Teniendo en cuenta que el contexto organizacional de esta guía y del MSPI en sí, son la Alcaldías del Estado, la metodología en la cual se basa la presente guía es la "Guía de Riesgos" del DAFP1, buscando que haya una integración a lo que se ha desarrollado dentro de la Alcaldía para otros modelos de Gestión, y de éste modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

Es así como alineando los Objetivos estratégicos de la Alcaldía, al desarrollo del MSPI se logra una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión por ejemplo el MECI2.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

Figura 7. Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: tomado de articles-150516_G7_Gestion_Riesgos

Figura 8. Niveles de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: tomado de articles-150516_G7_Gestion_Riesgos

ETAPAS SUGERIDAS PARA LA GESTIÓN DEL RIESGO

De acuerdo con lo señalado en la Guía de Gestión del Riesgo del DAFP (en adelante, la guía), se tienen tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la Alcaldía tener una administración de riesgos acorde con las necesidades de la misma.

De esta forma la primera y más importante para lograr un adecuado avance en todo el proceso de administración del riesgo es el "Compromiso de las alta y media dirección" puesto que al igual que como se menciona en la guía, tener el verdadero compromiso de los directivos garantizan en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona

en el MSPI la necesidad de tener aprobación de la dirección en cada etapa es necesaria.

Así mismo en concordancia con lo estipulado en la guía "debe designar a un directivo de primer nivel (debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del MECI y el Sistema de Gestión de la Calidad) que asesore y apoye todo el proceso de diseño e implementación del

Componente"3, el MSPI se acoge puesto que lo que se busca es lograr una gestión integral del riesgo.

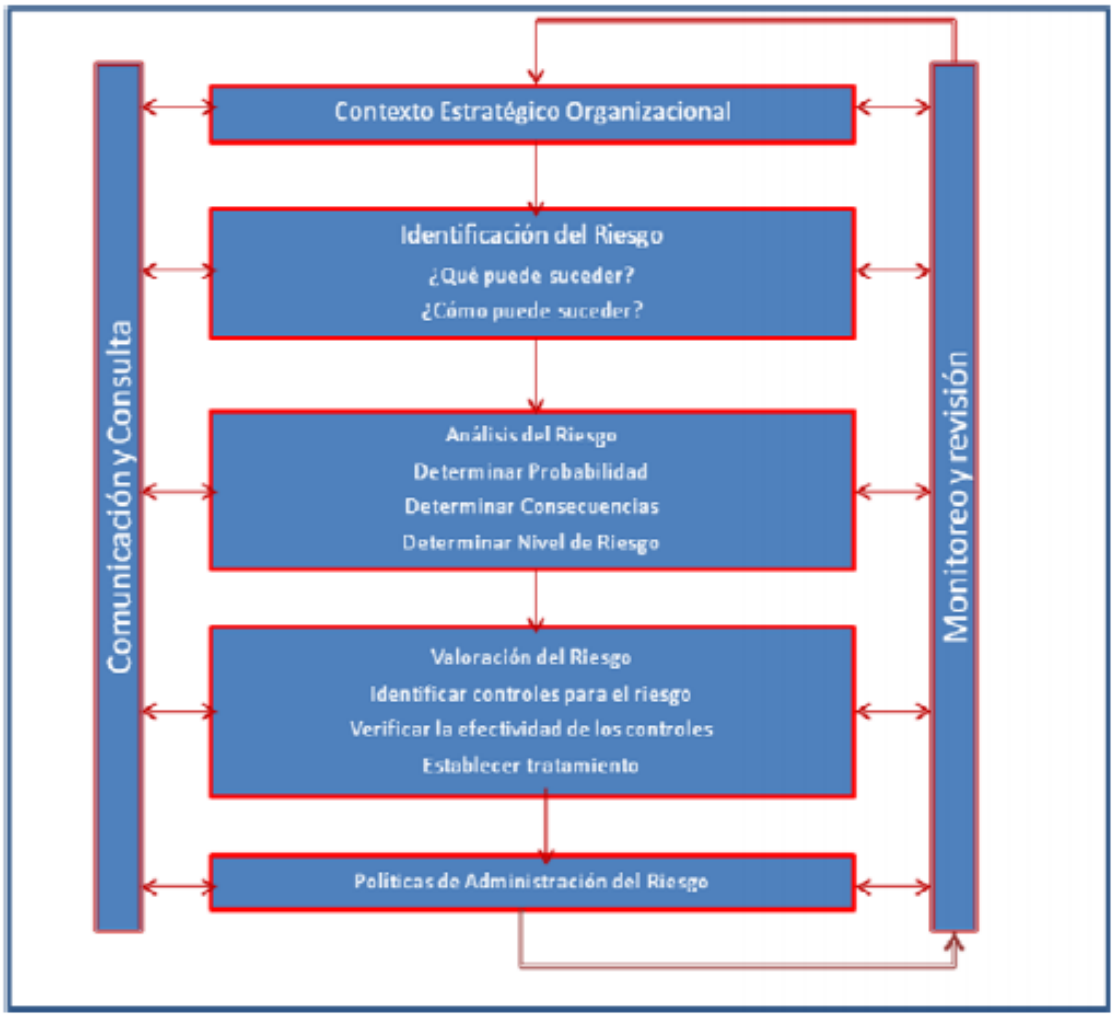
En segundo lugar se encuentra la "Conformación de un Equipo MECI o de un grupo interdisciplinario", la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la Alcaldía y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis para el MECI, o para el modelo de Gestión de Calidad.

Finalmente se encuentra la "Capacitación en la metodología", este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI, para tener un contexto Organizacional en todos los aspectos del desarrollo del MSPI.

VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

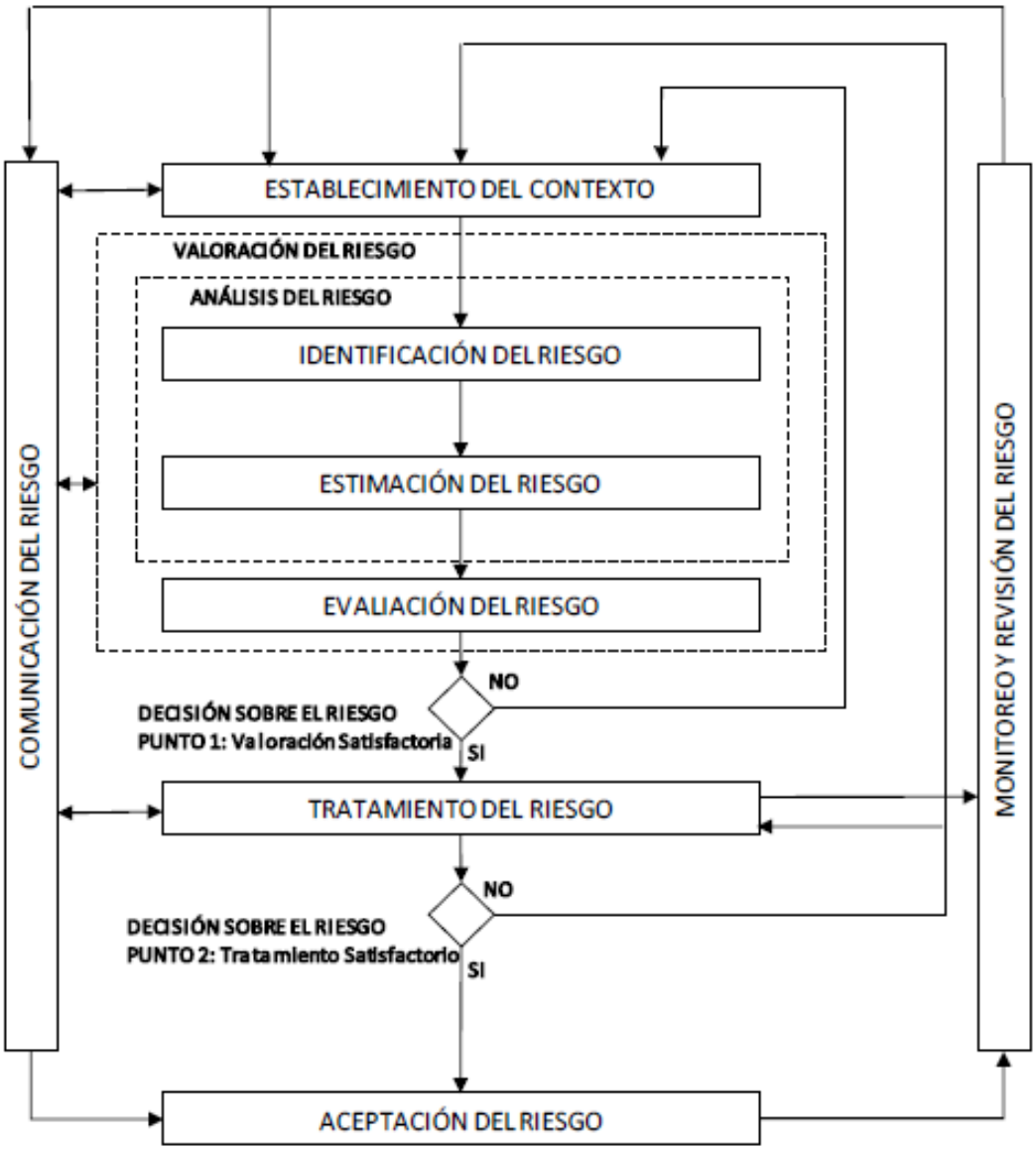
Figura 9. Visión general Administración de riesgo en seguridad de la información



Fuente: tomado de articles-150516_G7_Gestion_Riesgos

Proceso para la administración del riesgo en seguridad de la información

Figura 10. Proceso para la administración del riesgo en seguridad de la información



Fuente: tomado de articles-150516_G7_Gestion_Riesgos

Así como lo ilustra la imagen el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo

y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevara a cabo otra iteración de la valoración del riego con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la Alcaldía. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

Tabla 3. Actividades de Gestion de Riesgo – PHVA

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: tomado de articles-150516_G7_Gestion_Riesgos

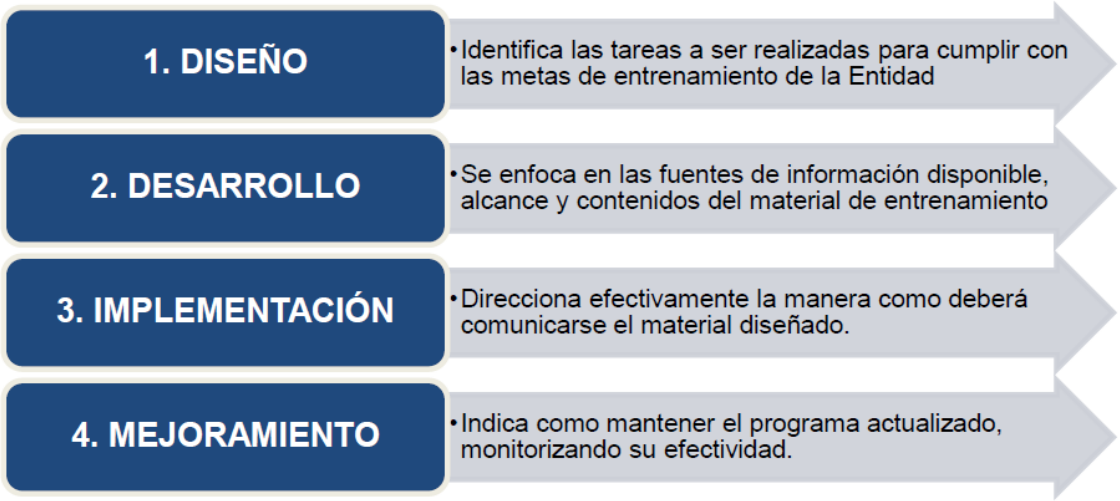
Para dar mayor profundidad al tema de identificación, valoración y tratamiento del riesgo la Alcaldía Municipal de Pasto hará uso de la Guia N° 7 Gestion de Riesgos.

PLAN DE COMUNICACIONES

Este apartado tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información de tal manera que le permita a la Alcaldía Municipal de Pasto asegurar que este abarque en su totalidad a los funcionarios de la Alcaldía de asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información de ser el caso.

Teniendo en cuenta lo anterior se presenta en la siguiente imagen donde se presenta las cuatro fases que se adoptaran para plantear e implementar el plan de comunicaciones.

Figura 11. Fases plan de sensibilización, capacitación y comunicación



Fuente: tomada de articles-5482_G14_Plan_comunicacion_sensibilizacion

Diseño, Desarrollo e Implementación

Con respecto a esta primera fase del plan de comunicaciones la Alcaldía Municipal de Pasto adoptara los temas propuestos en la guía articles-5482_G14_Plan_comunicacion_sensibilizacion mismo que se presenta en la siguiente figura.

Figura 12. Tematicas para sensibilización del personal de la Alcaldía Municipal de Pasto en Seguridad de la Información

Administración De Contraseñas	Uso Y Manejo De Inventario
Malware y sus diferentes tipos	Software Permitido/Prohibido En La Entidad
Políticas Organizacionales Relacionadas Con Seguridad De La Información	Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
Uso De Correo Electrónico E Identificación De Correos Sospechosos	Seguridad En El Puesto De Trabajo
Uso Apropiado De Internet	Temas de control de acceso a los sistemas (privilegios, separación de roles)
Política De Escritorio Limpio	**Ingeniería Social**
Sanciones Por Incumplimiento De Las Políticas	**Gestión De Incidentes (Como reportar, que puedo reportar)**
Spam	"Shoulder Surfing"
Backups Y Recuperación	Cambios En Los Sistemas
Amenazas Y Vulnerabilidades Comunes	Roles Y Responsabilidades En La Entidad

Fuente: tomada de articles-5482_G14_Plan_comunicacion_sensibilizacion

Tabla 4. Plan de Capacitación

N°	Actividad	Tema		Canal de Comunicación	Herramienta	Frecuencia	SEMANA 2 DICIEMBRE 2021
1	Jornada de Seguridad y Privacidad de la Informacion	**Administración De Contraseñas**	Uso Y Manejo De Inventario	Comunicación al interior de la Alcaldia	Piezas graficas	una vez al mes	
		Malware y sus diferentes tipos	Software Permitido/Prohibido En La Entidad				
		Politicas Organizacionales Relacionadas Con Seguridad De La Información	Uso De Dispositivos De La Entidad Fuera De Las Instalaciones				
		Uso De Correo Electrónico E Identificación De Correos Sospechosos	Seguridad En El Puesto De Trabajo				
		Uso Apropiado De Internet	Temas de control de acceso a los sistemas (privilegios, separación de roles)				
		Política De Escritorio Limpio	**Ingenieria Social**				
		Sanciones Por Incumplimiento De Las Políticas	**Gestión De Incidentes (Como reportar, que puedo reportar)**				
		Spam	"Shoulder Surfing"				
		Backups Y Recuperación	Cambios En Los Sistemas				
		Amenazas Y Vulnerabilidades Comunes	Roles Y Responsabilidades En La Entidad				

Fuente: propia

IMPLEMENTACIÓN CONTROLES ISO27001:2013

Tabla 5. Implementación controles ISO27001:2013

N°	Actividad	Tema	Canal de Comunicación	Herramienta	Frecuencia	SEMANA 2 FEBRERO 2022
1	IMPLEMENTACIÓN CONTROLES 27001:2013	* Implementación Controles 27001:2013	Comunicación al interior de la Alcaldia	ANEXO A ISO27001	SEMESTRAL	

Fuente: Propia

IMPLEMENTACION POLITICAS PRIMER Y SEGUNDO ORDEN SI

Tabla 6. Implementación política SI

N°	Actividad	Tema	Canal de Comunicación	Herramienta	Frecuencia	SEMANA 1 MARZO 2022
1	IMPLEMENTACION POLITICAS	IMPLEMENTACION POLITICAS SI	Comunicación al interior de la Alcaldia	POLITICAS SI	MENSUAL	

Fuente: Propia

PROCESOS CON METODOLOGÍA DE RIESGOS SI

Tabla 7. Proceso con metodología de riesgos SI

N°	Actividad	Tema	Canal de Comunicación	Herramienta	Frecuencia	SEMANAS DE TRABAJO FEBRERO MARZO 2022
1	PROCESOS CON METODOLOGIA RIESGOS SI	PROCESOS CON METODOLOGIA DE RIESGOS SI	Comunicación al interior de la Alcaldia	RIESGOS SI	MENSUAL	

Fuente: Propia

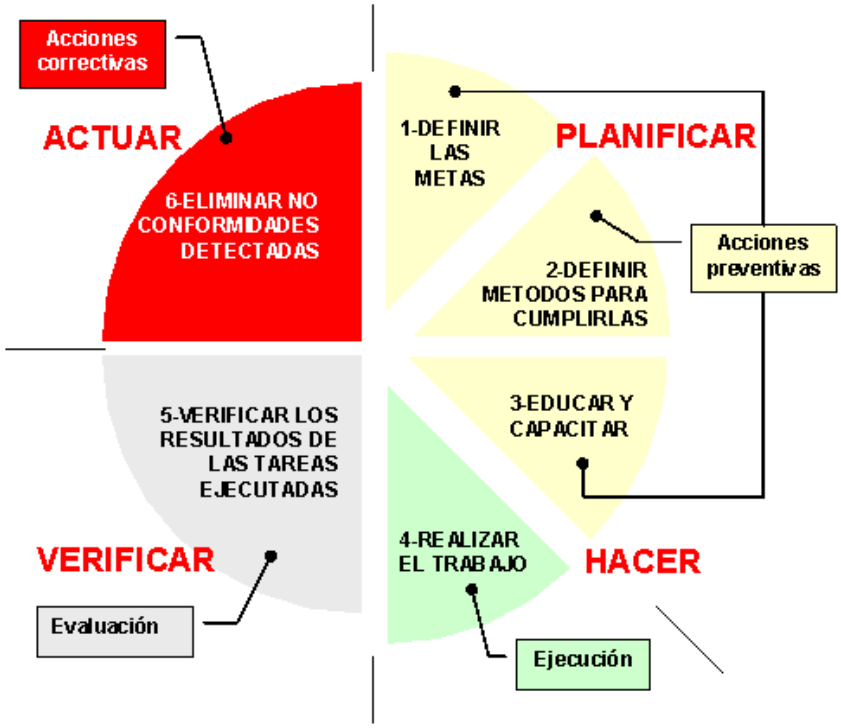
Alcance de la sensibilización

El alcance del plan de sensibilización está planteado para todo el personal de planta y contratistas de la Alcaldía Municipal de Pasto.

Mejoramiento Plan de Sensibilización

Para esta cuarta fase se implementara la metodología PHVA

Figura 13. Metodología PHVA



Fuente: Propia

Con el objetivo de mantener actualizado el plan de sensibilización midiendo su efectividad a través de evaluaciones al personal con las cuales se determinara la efectividad del mismo

Para tal fin se medirá el siguiente indicador:

Efectividad Plan Sensibilización SI = % apropiación del conocimiento

Fuente de información = Resultados Evaluaciones del personal

PLAN DE TRANSICION IPV4 A IPV6

INTRODUCCIÓN

Una de las herramientas importantes entre el mundo de la WEB y ahora en el nuevo mundo del INTERNET DE LAS COSAS es el servicio de internet, el cual es y será el principal medio para otorgar conexión a los nuevos dispositivos y para tal función las organizaciones deben tener en cuenta que la mayoría de los sistemas de Información implementados en las mismas necesitan de un direccionamiento IP.

Esta iniciativa va encaminada a la adopción del protocolo de internet versión 6 (IPv6) en la Alcaldía Municipal de Pasto esto en cumplimiento de la resolución 2710 para la implementación del protocolo IPV6 en Colombia buscando que la Alcaldías del Estado adopten el protocolo IPv6 en cada una de sus infraestructuras tecnológicas.

Por lo anterior, SE HACE NECESARIO Y UN DEBER que la Alcaldía Municipal de Pasto tenga en cuenta y ejecute según la disponibilidad de los recursos económicos la migración al protocolo IPv6 continuando con el crecimiento de la red y por ende garantizar el funcionamiento de software y hardware para el intercambio de información a nivel local y global.

Dentro del proceso de ejecución del contrato No. 2021XXX la Red Colombiana de Instituciones de Educación Superior – EDURED, como aporte a dicho convenio viene adelantando la actualización del PETI de la Alcaldía de Pasto y ha realizado el presente diagnostico con el propósito de apoyar al Municipio en el Proceso de actualización de la infraestructura tecnológica que permita soportar en sus equipos de seguridad perimetral el nuevo direccionamiento IPV6.

JUSTIFICACIÓN

Con el crecimiento en la cantidad de dispositivos móviles y despliegue de nuevas tecnologías y por ende la alta introducción de la conexión a internet y el reparto ineficiente de las direcciones disponibles ha generado escasez en el direccionamiento del protocolo de internet versión 4 (IPv4) usado para realizar las diferentes conexiones. Situación que se viene presentado a nivel mundial. Así lo dio a conocer el registro de direcciones de internet para América Latina y Caribe (LACNIC). Que sostiene que se llegó a una cuota de 6.002.688 direcciones IPv4 en su stock, con lo cual sólo podrán asignar cantidades muy pequeñas de direcciones IPv4.

La implementación de este protocolo IPv6 por parte de ALCALDÍA MUNICIPAL DE PASTO posibilitara que todos los dispositivos tecnológicos usados para la conexión a internet, tengan una dirección en IPv6. Facilitando así la conectividad en ancho de banda y a su vez ofrecer un mejor servicio a la comunidad ofreciendo mejores oportunidades para el desarrollo mundial.

La implementación del protocolo IPv6 para la ALCALDÍA MUNICIPAL DE PASTO es de suma importancia y urgencia ya que hará que este a la vanguardia de lo especificado y requerido en la actualidad permitiendo el acceso a un mayor número de aplicaciones de internet, pues si en una red sólo funciona el IPv4 no se

podrá acceder a ningún servicio que posea solamente el IPv6, lo que hará que la red se vuelva obsoleta.

Dentro del proceso de levantamiento del inventario de todo el equipamiento tecnológico realizado por EDURED, se identifica una seria deficiencia en los equipos de seguridad perimetral y de interconectividad de la infraestructura de fibra óptica que interconecta las diferentes sedes de la Alcaldía que se encuentran en una red WAN.

MARCO TEÓRICO

La transición a IPv6 ha sido impulsada por el Min TIC con la publicación de la Circular para la promoción de la adopción del IPv6 en Colombia en el año 2011, desde entonces se ha liderado un proceso de acompañamiento a Alcaldía en cada una de las etapas del proceso de migración.

A pesar de la escaza documentación de este tipo de procesos realizados con el Min TIC, se encuentra evidencia de transiciones a IPv6 realizados de manera autónoma en diversas instituciones educativas y otras organizaciones particulares. Se toman como referencia tres monografías, que, por su contenido similar al propuesto en la guía de transición, son de importancia para este proyecto.

"Diseño de la transición del protocolo ipv4 hacia ipv6 en la agencia colombiana para la reintegración- ACR con base en consideraciones de seguridad en implementación de ipv6." Diego Ferney Ramírez Pulido, Jaime Guzmán Pantoja, Jesús Alirio Beltrán Díaz. [10]

Se propone la transición a IPv6 en la ACR basándose en lineamientos dados por Gobierno En Línea (GEL 3.0), por Min TIC en la Circular 002 del 6 de Julio de 2011 y en la "Guía de transición de IPv4 a IPv6 para Colombia." De acuerdo con esto, se

realizan paso a paso las sugerencias propuestas en los documentos ya mencionados, es decir, se hace un plan diagnóstico y seguido se propone una estrategia para llevar a cabo la transición.

"MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6" Autores: Correa, Adelaida. Candamil, Martha Lucia1. Universidad Libre Facultad De Ingeniería De Sistemas. Bogotá 2010

El objetivo general de este proyecto fue planificar, implementar y emular los mecanismos de transición del protocolo IPV4 a IPV6 configurando y verificando los servicios de red sobre la plataforma 2003 Server Enterprise Edition Windows XP, y planificar los servicios de red utilizando los protocolos IPV4 e IPV6 que se puedan implementar en una red empresarial estándar.

"Propuesta de diseño para la transición del protocolo de internet versión 4 (IPv4) al protocolo de internet versión 6 (IPv6) en la ALCALDÍA MUNICIPAL DE PASTO. MARKET MIX S.A.S." Leidy Jesneth Melo Moreno. [11]

Se desarrolla un modelo para la migración de los protocolos de internet, de IPv4 a IPv6, que sirva de guía para las personas que pretendan desarrollar este proceso dentro de una PYME (Pequeña y Mediana Empresa); teniendo en cuenta el análisis y la propuesta de una estrategia basados en la operatividad y necesidades la ALCALDÍA MUNICIPAL DE PASTO. MARKET MIX S.A.S. Como primer paso se realiza apología y el diagrama lógico de la red de comunicaciones; seguido a ello se muestra la metodología para la transición dividida en cuatro fases. La primera hace referencia a la investigación sobre información existente del tema, la segunda implica el diseño general del sistema, teniendo en cuenta protocolos de enrutamiento y otros aspectos técnicos; la siguiente fase involucra la revisión de requisitos de arquitectura y la identificación de los recursos que

dependen de IPv4; la última fase es la adquisición de hardware y software, el formato general de la interfaz, el modelo propuesto para la infraestructura y la adquisición de un bloque de direcciones IPv6.

FUNDAMENTOS TEÓRICOS

Red de datos

También llamada red de computadoras, red de comunicaciones o red informática, es el conjunto de elementos de hardware y software informático conectados a través de dispositivos físicos que permitan el envío y la recepción de datos con el fin de compartir información, recursos y servicios. De acuerdo al alcance de transmisión de los datos, puede ser red de área local o LAN, red de área metropolitana o MAN, red de área extensa o WAN. Algunas clases de redes de datos de acuerdo con su topología o diseño, pueden ser

Topología de Bus: Usa un solo cable backbone que debe terminarse en ambos extremos. Todos los host se conectan directamente a este backbone.

Topología de anillo: Conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable

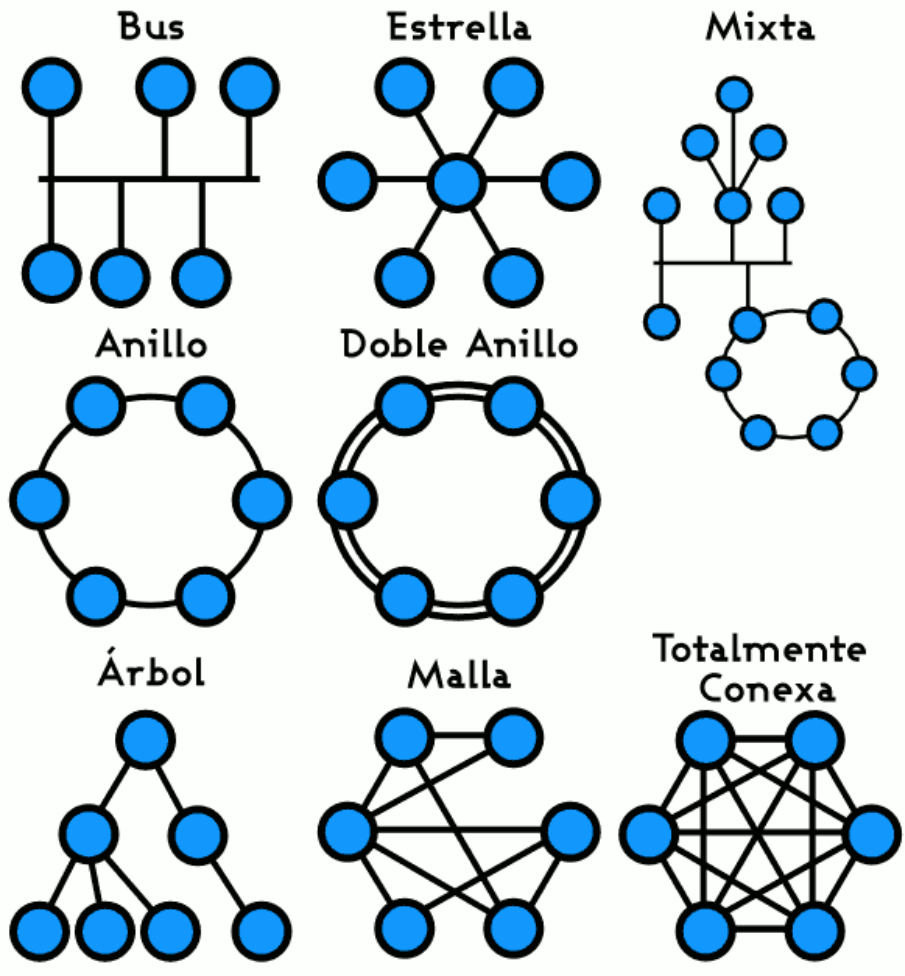
Topología de estrella: Conecta todos los cables con un punto central de concentración.

Topología de estrella extendida: Conecta estrellas individuales entre si mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

Topología jerárquica: Es similar a la de una estrella extendida. Pero en lugar de conectar hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

Topología de malla: Se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio

Figura 14. Tipologías de red



Fuente: Tipo de Redes de datos tomada de https://www.google.com/search?q=tipos+de+redes+de+datos&sxsrf=AOaemvIRjY

2l4pWZA5mSeWq_odhohrWX5Q:1636403145025&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjCi6zhzln0AhWzTjABHWZlBM4Q_AUoAXoECAEQAw&biw=1366&bih=617&dpr=1#imgrc=4f4dHr_qYlEgWM

PROTOCOLO DE INTERNET VERSIÓN 4 O IPV4

Sistema de identificación que se utiliza en internet para enviar información entre dispositivos, la cuarta es la versión más utilizada del protocolo. Éste asigna una serie de cuatro números, cada uno de ellos comprendido entre 0 y 255, por lo tanto, cada dirección es de 32 bits y sólo permite aproximadamente 4.000 millones de direcciones únicas, las cuales entraron en proceso de agotamiento desde hace varios años

DIRECCIONES IPV4

Como referencia5 para entender el por qué el espacio de direcciones IPv4 es limitado a 4.3 mil millones de direcciones, se puede descomponer una dirección IPv4. Una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal, separados por puntos. Un bit puede ser tanto un 1 como un 0 (2 posibilidades), por lo tanto, la notación decimal de un octeto tendría 2 elevado a la 8va potencia de distintas posibilidades (256 de ellas para ser exactos). Ya que se empieza a contar desde el 0, los posibles valores de un octeto en una dirección IP van de 0 a 255.

Ejemplos de direcciones IPv4: 192.168.0.1, 66.228.118.51, 173.194.33.16

Figura15. Ejemplos dirección IPV4

FUENTE: Funcionamiento de IPV4 tomada de https://www.google.com/search?q=funcionamiento+ipv4&tbm=isch&ved=2ahUKEwiR4sr6zIn0AhVRPN8KHVk7AAUQ2-cCegQIABAA&oq=funcionamiento+ipv4&gs_lcp=CgNpbWcQAzIECAAQGDoHCCMQ7wMQJzoECAAQQzoFCAAQgARQlwxYkhlgmxtoAHAAeACAAcYBiAH6E5IBBDAuMTaYAQCgAQGqAQtnd3Mtd2l6LWItZ8ABAQ&sclient=img&ei=_YeJYdHvOdH4_AbZ9oAo&bih=617&biw=1366#imgrc=UGP8FCgMVqzT1M

PROTOCOLO DE INTERNET VERSIÓN 6 O IPV6

Protocolo de Internet de última generación, diseñado en los años 90 por el IETF para sustituir a IPv4. A diferencia de la anterior versión, en esta las direcciones se

componen de 128 bits, lo que permite la existencia de aproximadamente 340 billones de direcciones IP únicas.

DIRECCIONES IPV6

Las direcciones IPv6 tienen un tamaño de 128 bits, distribuidos en ocho campos de dieciséis bits representados por cuatro números hexadecimales cada uno y separados por dos puntos. En la figura 2 se puede observar el formato de una dirección IPv6, los cuarenta y ocho primeros bits, es decir, los tres primeros campos contienen el prefijo de sitio, éste describe la topología pública y es el segmento que suelen asignar al sitio los ISP o RIR (Registro Regional de Internet). Los siguientes dieciséis bits lo ocupa el ID de subred y describe la topología privada, es asignado por el administrador de la red. Los últimos sesenta y cuatro bits, o cuatro campos de la derecha, contienen el ID de interfaz y se puede configurar manual o automáticamente.

CLASES DE DIRECCIONES IPV6

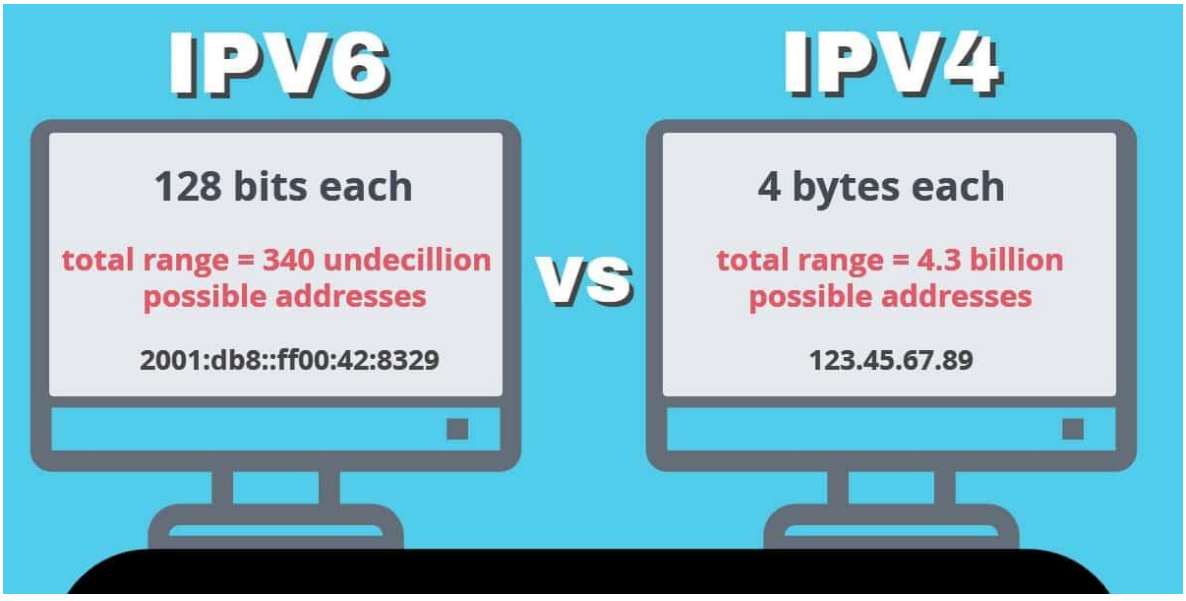
Direcciones de unidifusión. Identifica una interfaz de un solo nodo. Pueden ser de unidifusión global, de transición o local de vínculo, las primeras son globalmente exclusivas de internet y en IPv4 serían las mismas IP públicas; las direcciones de transición son las que llevan incrustadas en ellas una dirección IPv4 con el fin de facilitar técnicas de migración como los túneles en el proceso de transición; finalmente, las direcciones locales de vínculo se utilizan en las relaciones de red local, no son válidas ni se reconocen fuera del ámbito corporativo u organizativo, en IPv4 equivaldrían a las IP privadas.

Direcciones de multidifusión. Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección multidifusión se dirigen a todos los miembros del grupo de multidifusión.

Direcciones de difusión por proximidad. Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección de difusión por proximidad se dirigen al nodo de miembros del grupo de difusión que se encuentre más cerca del remitente

CARACTERÍSTICAS IPV4 VS IPV6

Figura 16. CARACTERISTICAS IPV4 VS IPV6



FUENTE: Características de protocolos tomada de https://www.google.com/search?q=ipv4+vs+ipv6&tbm=isch&ved=2ahUKEwjVrdqHzYn0AhXwAt8KHaCRCEcQ2-

cCegQIABAA&oq=ipv4+vs+ipv6&gs_lcp=CgNpbWcQAzIECAAQQzIFCAAQgAQyBQgAEIAEMgQIABAeMgQIABAeMgQIABAeMgQIABAeMgQIABAeMgQIABAeOgcIIxDvAxAnOggIABCABBCxAzoHCAAQsQMQQ1DGC1j3KWCrLGgAcAB4AIAB0gGIAdMPkgEGMC4xMi4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=GYiJYZW9HPCF_Aago6K4BA&bih=617&biw=1366#imgrc=KOMoAAFmQctBTM

PROTOCOLO TCP/IP

TCP/IP3 (Transmission Control Protocol/Internet Protocol), más que un protocolo, TCP/IP es un conjunto de protocolos de red, capaces de soportar las comunicaciones entre equipos conectados a gran número de redes heterogéneas, independientes de un vendedor. Su origen es: solucionar las comunicaciones a través de la red ARPANET para el Departamento de Defensa de USA (Departament of Defense 1.972). Comienza su utilización en DARPA (Agencia de proyectos de investigación avanzada para la defensa).

TECNOLOGÍA A IMPLEMENTAR PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6)

Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los noventa por parte del Internet Engineering Task Force, en adelante IETF por sus siglas en inglés. Al día de hoy, el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente robusto y maduro para soportar la operación del internet en substitución de IPv4.

De otro lado, el IPv6 representa quizás el cambio más importante en la historia del internet, ya que es necesario para que la red de redes pueda seguir

desarrollándose de una forma segura y estable, gracias a que tiene un espacio de direcciones de 128 bits y, por tanto, puede direccionar 2^128 interfaces de red (340.282.366.920.938.463.463.374.607.431.768.211.456)

CARACTERÍSTICAS DE IPV6

Las características del IPv6 son las siguientes:

- Cantidad de Direcciones
- Asignación y flexibilidad Global (Sin NAT)
- Calidad de servicio QoS
- Arquitectura jerárquica de direcciones
- Soporte a tráfico multimedia en tiempo real
- Autoconfiguración de equipos
- Computación móvil
- Seguridad e integridad de datos
- Aplicaciones Multicast y Anycast
- Mecanismos de transición gradual de IPv4 a IPv6

POLÍTICAS DE ENRUTAMIENTO IPV6

El plan de enrutamiento para IPv6 no debe variar en demasía sobre lo que ya se hace en IPv4. En general para una empresa tiene sentido que en IPv6 se

mantenga la misma topología que en IPv4, pues el mantener dos topologías significaría incrementar el costo de operación del encaminamiento de la red y el aumento de incidentes. Las opciones de enrutamiento en IPv6 son:

Enrutamiento estático.

Enrutamiento dinámico, en éste existen distintas categorías, como protocolos de vector distancia ó RIPNG (RIP Next Generation), protocolos de vector camino ("path vector") ó BGPv4 y protocolos de estado de enlaces: ISIS o u OSPFv3. Con todas estas opciones, se debe considerar especialmente el enrutamiento ya existente en la compañía. En caso de estar utilizando OSPFv2 para la red IPv4, tiene sentido utilizar OSPFv3 en IPv6, al igual que utilizar BGPv4 para el encaminamiento externo. En caso de utilizar direccionamiento estático para IPv4, se puede utilizar las mismas configuraciones para IPv6.

MECANISMOS DE TRANSICIÓN.

La versión 6 del Protocolo de Internet ha sido diseñada para que su implementación se realice en coexistencia con IPv4. A continuación, se describen algunas de las principales categorías de mecanismos que facilitarían dicha migración; estos pueden ser utilizados solos o en combinación y la migración puede ser realizada paso a paso, comenzando con un solo nodo, de igual manera puede darse el caso en el que la red completa sea migrada a IPv6 mientras que el proveedor de servicios siga utilizando IPv4, o puede darse el caso contrario.

DOBLE PILA.

Tanto en nodos como en enrutadores se tendrá un soporte IPv4 e IPv6, por lo tanto, tienen la habilidad de enviar y recibir paquetes de los dos protocolos. Un

nodo trabajando con este mecanismo puede operar de las siguientes maneras: • Con la pila IPv4 habilitada pero la pila IPv6 deshabilitada. • Con la pila IPv6 habilitada pero la pila IPv4 deshabilitada. • Con las dos pilas habilitadas. La desventaja de este mecanismo es que necesita tener tablas de enrutamiento y soporte para ambos protocolos.

TÚNELES

Por medio de este mecanismo se utiliza la infraestructura de enrutamiento IPv4 para llevar los paquetes IPv6, hasta que toda la infraestructura se encuentre con el nuevo protocolo. Cada túnel puede ser implementado de diferente manera: • Enrutador a enrutador. Los enrutadores IPv6/IPv4 interconectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos. • Host a enrutador: Los host IPv6/IPv4 pueden tunelizar paquetes IPv6 a un enrutador IPv6/IPv4 por medio de una infraestructura IPv4. • Host a host. Los host IPv6/IPv4 que están conectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos mismos.

DESCRIPCIÓN DEL PROBLEMA

Las organizaciones públicas y privadas se encuentran ante una gran problemática debido a la gran reducción del número de direcciones IPv4 a causa de la población que hace uso del servicio de internet teniendo en cuenta no solo los computadores o equipos de oficina, sino también; los dispositivos móviles como Smartphones y/o tabletas.

Actualmente la Alcaldía de Pasto cuenta con un equipamiento tecnológico que permite todo el enrutamiento lógico y físico de comunicaciones de voz, datos y video que fue adquirido en el mes de noviembre del año 2014 según el contrato No. 20142510, los cuales mantiene en servicio las 24 horas del días, los 7 días de la

semana durante los 12 meses del año, de forma permanente, estos dispositivos de operación critica cumplieron en el mes de noviembre de 2021, siete años de funcionamiento continuo y entrando en un proceso de obsolescencia tecnológica y sin contar actualmente con garantía y/o soporte técnico que permitan garantizar en caso de fallo el remplazo de forma inmediata sin generar traumatismos en el proceso de migración al protocolo IPV6 y que no genere ningún tipo de indisponibilidad en todos los servicios que operan dentro de la Alcaldía de Pasto y que están prestando los diferentes servicios a toda la población del Municipio de Pasto.

OBJETIVO GENERAL

Definir el plan de transición de protocolo de internet IPV4 a IPV6 en las diferentes sedes de la ALCALDÍA MUNICIPAL DE PASTO, según el levantamiento y actualización del inventario de equipos de comunicación que permitan soportar la migración al nuevo esquema de direccionamiento IP requerido por la Alcaldía.

3.2 OBJETIVOS ESPECÍFICOS

- Recopilar información de los dispositivos de tecnología en la ALCALDÍA MUNICIPAL DE PASTO.
- Recopilar información de los dispositivos de comunicaciones en la ALCALDÍA MUNICIPAL DE PASTO.
- Recopilar información de las aplicaciones y plataformas que se usan en la ALCALDÍA MUNICIPAL DE PASTO.
- Recopilar información de la topología de red.

- Presentar el diagnóstico del estado de los equipos de seguridad perimetral de la ALCALDÍA MUNICIPAL DE PASTO.

DISEÑO METODOLÓGICO

Metodología

La metodología utilizada es el ciclo continuo PHVA ya que permite el mantenimiento y mejora continua dentro de cualquier organización y la cual se utilizada para el proceso de transición de IPV4 A IPV6

Figura 17. Metodologia PHVA

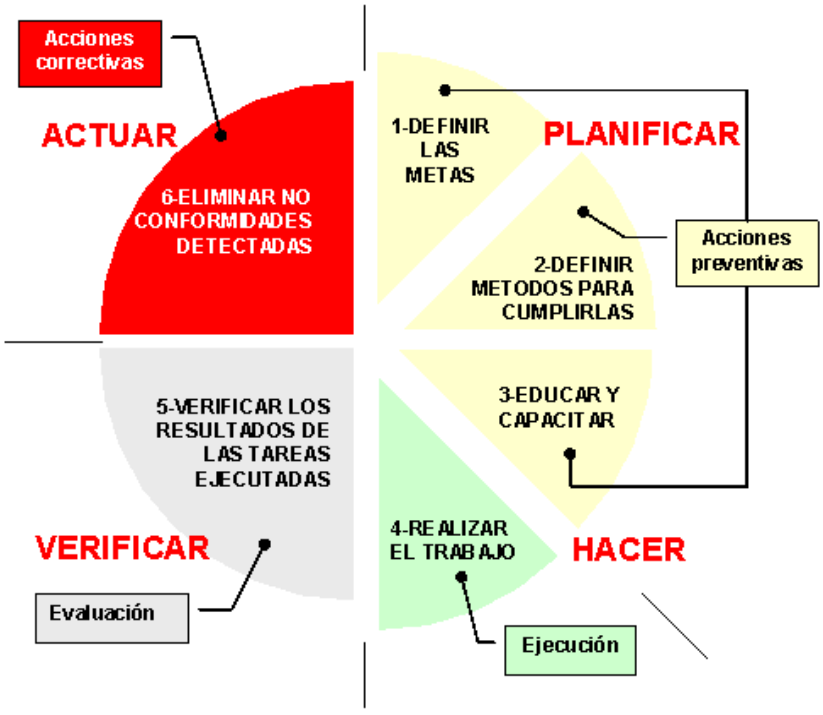


Ilustración 6- Modelo PHVA tomada de https://www.google.com/search?q=ciclo+phva&tbm=isch&ved=2ahUKEwjY1eCmzYn0AhWLnOAKHa8gDFQQ2-cCegQIABAA&oq=ciclo+phva&gs_lcp=CgNpbWcQAzIICAAQgAQQsQMyCAgAEIAEELEDMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQ6BwgjEO8DECc6BggAEAcQHjoECAAQHjoECAAQQzoHCAAQsQMQQ1DECliCH2DQIGgBcAB4AIABsQGIAcQOkgEEMC4xMpgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=WoiJYdjAI4u5ggevwbCgBQ&bih=617&biw=1366#imgrc=KWEje9v6rRt9-M

Planificar: En la etapa de planificación se establecen objetivos y se identifican los procesos necesarios para lograr unos determinados resultados de acuerdo a las políticas de la organización. En esta etapa se determinan también los parámetros de medición que se van a utilizar para controlar y seguir el proceso.

Hacer: Consiste en la implementación de los cambios o acciones necesarias para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un plan piloto a modo de prueba o testeo.

Verificar: Una vez se ha puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la efectividad de los cambios. Se trata de una fase de regulación y ajuste.

Actuar: Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

Etapas De Implementación

Tabla 8. Etapa Plan De Diagnostico IPV6

Fase 1	Actividad	Responsable
Diagnóstico de la Situación Actual de Empopasto	Construcción del plan de Diagnóstico.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Inventario de TIC.	EDUIRED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Análisis de la topología de la infraestructura.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN

	Planeación de la transición de los servicios tecnológicos de la Alcaldía.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Validación de estado de los sistemas de información, los sistemas de comunicaciones.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Identificación de esquemas de seguridad de la información y las comunicaciones.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN

Fuente: Creación propia

Tabla 9. Etapa De Implementación

Fase 2	Actividad	Responsable
	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	EDURED - SUBSECRETARIA DE SISTEMAS DE

		INFORMACIÓN
Desarrollo del Plan de implementación	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en los equipos a emplear direccionamiento IP.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Coordinación con el proveedor de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN

Fuente: Creación propia

Tabla10. Etapa De Pruebas De Funcionalidad De IPV6

Fase 3	Actividad	Responsable
	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Alcaldía.	EDURED - SUBSECRETARIA DE SISTEMAS DE

Pruebas de funcionalidad de IPv6		INFORMACIÓN
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN
	Afinamiento de las configuraciones de hardware, software y servicios de la Alcaldía.	EDURED - SUBSECRETARIA DE SISTEMAS DE INFORMACIÓN

Fuente: Creación propia

FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del Modelo de Seguridad y Privacidad de la Información por parte de la Alcaldía Municipal de Pasto se hará tomando como base los resultados que arrojan los indicadores propuestos para la verificación de la efectividad, la eficiencia y la eficacia de las acciones respectivas a la seguridad de la información.

Figura 18. Fase de evaluación de desempeño

Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

De igual manera como en las anteriores fases la Alcaldía Municipal de Pasto tendrá en cuenta la siguiente tabla donde se plantean las metas, resultados e instrumentos a utilizar para la ejecución de la fase de de evaluación y desempeño.

Tabla 11. Metas, Resultados e Instrumentos de la fase de Evaluación de Desempeño

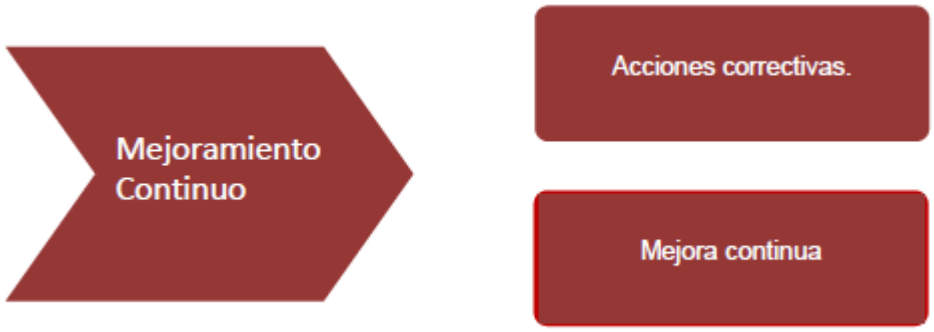
Evaluación del Desempeño			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría.	

Fuente: Fuente: tomada de la guía Modelo de Seguridad y Privacidad de la Información

FASE MEJORA CONTINUA

En esta fase la Alcaldía Municipal de Pasto consolidara los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Figura 20. Fases Mejora continúa



Fuente: Tomada del Modelo de Seguridad y Privacidad de la Información

Para el cumplimiento de las metas de esta fase se adopta las siguientes metas identificadas en la siguiente tabla

Tabla 12. Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua			
Metas	**Resultados**	**Instrumentos**	
		MSPI	**MRAE**
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

Fuente: Tomada del Modelo de Seguridad y Privacidad de la Información.

FASE DE IMPLEMENTACION

Figura 21. Fase de implementación

Fuente: Guía – Modelo de Seguridad y privacidad de la información.

Implementación del plan de tratamiento de riesgos

El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002. El documento presenta los objetivos de control del estándar ISO 27002. La información es un recurso que, como el resto de los activos, tiene valor para el organismo y por consiguiente debe ser debidamente protegida. Las políticas de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de

garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos[1]

Para tal fin la Alcaldía Municipal de Pasto acoge lo estipulado por el MINTIC de tomar como base la Guía N8. De controles de Seguridad y Privacidad del MSPI

Indicadores de Gestión.

Para realizar la medición de la implementación del MSPI al interior de la Arcadia Municipal de Pasto se adoptan los indicadores propuestos en la Guía N9 – Indicadores de Gestión de Seguridad de la Información que analizados se alinean al actual funcionamiento del proceso de Gestión de Tecnologías de la Información y son acordes susceptibles actualizaciones de dicho procedimiento.

¡ El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

---

1 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150511_G8_Controles_Seguridad.pdf